ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

JEAN COUGNARD

Nouveaux exemples d'extension relatives sans base normale

Annales de la faculté des sciences de Toulouse 6e série, tome 10, nº 3 (2001), p. 493-505

<http://www.numdam.org/item?id=AFST_2001_6_10_3_493_0>

Annales de la Faculté des Sciences de Toulouse Vol. X, n° 3, 2001
pp. 493–505

Nouveaux exemples d'extension relatives sans base normale (*)

JEAN COUGNARD (1)

RÉSUMÉ. — En améliorant des résultats antérieurs de I. Brinkhuis et de l'auteur, on donne de nouveaux exemples d'extensions cycliques relatives modérément ramifiées dont l'anneau des entiers ne possède pas de base normale.

ABSTRACT. — Using earlier works of I. Brinkhuis and the author we give new examples of relative cyclic tame extensions of number fields without normal integral bases.

1. Introduction

Soit N/k une extension galoisienne de corps de nombres, H son groupe de Galois, O_k l'anneau des entiers de k, O_N celui de N. Si on suppose N/k modérément ramifiée (i.e. les indices de ramification sont premiers aux caractéristiques des corps résiduels correspondants) O_N est un $O_k[H]$-module projectif. La question se pose de savoir s'il est libre. Un cas particulier est pointé par A. Fröhlich :

Soit p, ℓ deux nombres premiers impairs, $p \equiv 1 \bmod \ell$, $N = \mathbb{Q}(\zeta_p)$ le p-ème corps cyclotomique, k le sous-corps de $\mathbb{Q}(\zeta_p)$ de degré $\frac{p-1}{\ell}$ sur $\mathbb{Q}$ et $H = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/k)$. Il est montré dans [B1], [C], [B2] que $\mathbb{Z}[\zeta_p]$ n'est pas $O_k[H]$-libre. Dans [C] et [B2] cette question est étudiée lorsque $\frac{p-1}{\ell}$ est premier à ℓ. On se propose de démontrer que les techniques utilisées permettent de mettre en évidence d'autres extensions relatives dont l'anneau

(*) Reçu le 19 mars 2001, accepté le 15 octobre 2001

(1) FRE 2271 C.N.R.S., U.F.R. Sciences Université de Caen, Campus II, Bd Mal. Juin, B.P. 5681, 14032 Caen Cedex.
courriel : cougnard@math.unicaen.fr

des entiers n'est pas libre (s'agissant d'extensions abéliennes, stablement libre équivaut à libre).

On conserve les données p et ℓ premiers impairs, on pose $p-1=\ell^a m$ avec $(\ell,m)=1$, $a\geqslant 1$; $k/\mathbb{Q}$ est cyclique de degré $n=p^b n_0$ $((n_0,p\ell)=1)$ ramifiée totalement en p (donc $n_0|p-1$). On considère K le sous-corps, de degré ℓ sur $\mathbb{Q}$, du p-ème corps cyclotomique ; on construit $N=Kk$ (K et k sont linéairement disjoints sur $\mathbb{Q}$) et on pose $G=\mathrm{Gal}(N/K)\simeq\mathrm{Gal}(k/\mathbb{Q})$, $H=\mathrm{Gal}(N/k)\simeq\mathrm{Gal}(K/\mathbb{Q})$. Enfin, on fait l'hypothèse :

(H) *ℓ n'est pas ramifié dans $k/\mathbb{Q}$.*

On se propose de démontrer :

THÉORÈME 1.— *Avec les notations précédentes et l'hypothèse (H), si $\mathcal{M}$ est l'ordre maximal de $k[H]$ et si $\mathcal{M}O_N$ est $\mathcal{M}$-libre alors k est l'un des corps $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{-p})$.*

THÉORÈME 2.— *Avec les notations précédentes et l'hypothèse (H), O_N n'est pas $O_k[H]$-libre.*

Dans le théorème 1, lorsque $k=\mathbb{Q}(\sqrt{-p})$ C. Greither (cf. [Gr]) montre qu'il existe de nombreux exemples où $\mathcal{M}O_N$ est effectivement $\mathcal{M}$-libre. Ses méthodes n'ont pas permis de mettre en évidence des contre-exemples.

Dans le second paragraphe on rappelle brièvement la description du groupe des classes des $O_k[H]$-modules localement libres.

Dans le paragraphe suivant on décrit l'invariant associé à O_N. Dans le paragraphe 4, on regarde ce que devient l'anneau O_N lorsque l'on étend les scalaires à l'ordre maximal de $O_k[H]$, en exploitant la technique utilisée dans [C] ; ceci suffit à donner de nouvelles familles d'anneaux d'entiers localement libre mais non libres et nous ramène au cas où $[k:\mathbb{Q}]$ est une puissance de 2.

Dans la cinquième partie, on reprend alors les idées de [B2], on en déduit que si O_N étendu à l'ordre maximal est libre, k est l'un des deux corps de théorème 1. On termine par la démonstration du théorème 2.

L'anneau des entiers O_K est $\mathbb{Z}[H]$-libre avec une base qui peut être choisie égale à $\theta=\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p)$. On note $\mathcal{P}$ (resp. $\mathcal{P}'$, $\mathcal{P}''$) l'unique idéal premier au-dessus de p dans k (resp. K, N), l'extension N/k est ramifiée uniquement (et modérément) en $\mathcal{P}$; on en déduit que θ engendre une base locale de O_N comme $O_k[H]$-module pour toute place de O_k différente de $\mathcal{P}$. Localisé en $\mathcal{P}$, O_N est aussi libre sur $O_{k_\mathcal{P}}[H]$, on note $a_\mathcal{P}$ une base locale en cette place.

On a besoin d'adjoindre les racines ℓ-èmes de l'unité aux corps déjà cités. L'hypothèse de ramification faite en ℓ implique la disjonction linéaire de $\mathbb{Q}(\zeta_\ell)$ et N sur $\mathbb{Q}$. Pour tout corps M, on note $M^{(\ell)} = M(\zeta_\ell)$ le corps obtenu en adjoignant à M les racines ℓ-èmes de l'unité. On fait donc intervenir $\mathbb{Q}^{(\ell)}$, $K^{(\ell)}$, $k^{(\ell)}$, $N^{(\ell)}$. Puisque $p \equiv 1 \bmod \ell$, les idéaux, $(p), \mathcal{P}, \mathcal{P}', \mathcal{P}''$ se décomposent dans les corps obtenus en adjoignant les racines ℓ-èmes de l'unité. On note $\mathcal{P}'' O_{N^{(\ell)}} = \mathfrak{P}_1'' \dots \mathfrak{P}_{\ell-1}''$, et $\mathfrak{P}_i = \mathfrak{P}_i'' \cap k^{(\ell)}$, $\mathfrak{P}_i' = \mathfrak{P}_i'' \cap K^{(\ell)}$, $\mathfrak{p}_i = \mathfrak{P}_i'' \cap \mathbb{Q}^{(\ell)}$.

Comme ℓ et p sont premiers entre eux les extensions $K^{(\ell)}//\mathbb{Q}^{(\ell)}$, $N^{(\ell)}//k^{(\ell)}$ sont modérément ramifiées et les bases normales globales (resp. locales) de $K/\mathbb{Q}$ (resp. N/k) le restent après adjonction des racines de l'unité.

2. Groupe des classes projectives

On rappelle, dans ce cadre, la description donnée par Fröhlich ([F], appendice 1). Soit R_H le groupe des caractères virtuels de H, $N^{(\ell)}$ le corps contenant l'extension étudiée et les valeurs des caractères de H, $J(N^{(\ell)})$ son groupe des idèles, $\Omega = \mathrm{Gal}(N^{(\ell)}/k)$. Le groupe multiplicatif $N^{(\ell)*}$ de $N^{(\ell)}$ s'envoie de manière diagonale dans $J(N^{(\ell)})$. Si $\mathcal{S}$ est l'ensemble des places de k, le produit $\prod_{\mathfrak{q}\in\mathcal{S}} \left(O_{k_\mathfrak{q}}[H]^*\right)$ est isomorphe au groupe $\mathrm{Det}\left(U(O_k[H])\right)$ de l'appendice I de [F], il peut être considéré comme un sous-groupe de $\mathrm{Hom}_\Omega(R_H, J(N^{(\ell)}))$. On a alors l'isomorphisme :

$$\mathrm{Cl}(O_k[H]) \simeq \frac{\mathrm{Hom}_\Omega(R_H, J(N^{(\ell)}))}{\mathrm{Hom}_\Omega(R_H, N^{(\ell)*}) \prod_{\mathfrak{q}\in\mathcal{S}} \left(O_{k_\mathfrak{q}}[H]^*\right)}$$

Le groupe des classes projectives de l'ordre maximal $\mathcal{M}$ contenant $O_k[H]$ est :

$$\mathrm{Cl}(\mathcal{M}) \simeq \frac{\mathrm{Hom}_\Omega(R_H, J(N^{(\ell)}))}{\mathrm{Hom}_\Omega(R_H, N^{(\ell)*})\mathrm{Hom}_\Omega\left(R_H, U(J(N^{(\ell)}))\right)}$$

où dans le dénominateur $U(\ )$ indique le groupe des idèles qui sont des unités en toute place finie. Par évaluation des idèles en idéaux, ce groupe est isomorphe au produit des groupes des classes $\mathrm{Cl}(k) \times \mathrm{Cl}(k^{(\ell)})$. On sait, puisque l'extension N/k est modérément ramifiée que la trace de O_N est O_k donc un O_k-module libre. La classe (O_N) de O_N se trouve ainsi dans le noyau $\mathcal{K}$ du morphisme :

$$\mathrm{Cl}(O_k[H]) \simeq \frac{\mathrm{Hom}_\Omega(R_H, J(N^{(\ell)}))}{\mathrm{Hom}_\Omega(R_H, N^{(\ell)*}) \prod_{\mathfrak{q}\in\mathcal{S}} \left(O_{k_\mathfrak{q}}[H]^*\right)} \longrightarrow \frac{J(k)}{k^* U(J(k))} \simeq \mathrm{Cl}(k)$$

obtenu en restreignant les applications au caractère trivial. Les hypothèses de ramification en p et ℓ font que les autres caractères forment une seule orbite sous l'action de Ω. Le noyau de cet homomorphisme se calcule au moyen du diagramme suivant :

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \mathcal{G} & \longrightarrow & J(k^{(\ell)}) & \longrightarrow & \mathcal{K} \\
 & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \mathrm{Hom}_\Omega(R_H, N^{(\ell)*})\prod_{\mathfrak{q}\in S} O_{k\mathfrak{q}}[H]^* & \longrightarrow & \mathrm{Hom}_\Omega(R_H, J(N^{(\ell)})) & \longrightarrow & \mathrm{Cl}(O_k[H]) \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & k^*\prod_{\mathfrak{q}\in S} U(O_{k_\mathfrak{q}}) & \longrightarrow & J(k) & \longrightarrow & \mathrm{Cl}(k) \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 1 & & 1 & & 1
\end{array}$$

où le terme du milieu de la suite des noyaux vient de l'action de Ω sur R_H et sur les groupes d'idèles. Le noyau recherché est celui de droite de la même ligne, il est isomorphe à $J(k^{(\ell)})/\mathcal{G}$. Le groupe $\mathcal{G}$ est formé des fonctions fg où f est une fonction équivariante de R_H dans $k^{(\ell)}$ et g une fonction équivariante définie, pour chaque caractère, par ses composantes locales : $g_\mathfrak{p}(\chi) = \chi(\sum_{h\in H} a_{\mathfrak{q},h}h)$ avec $\sum_{h\in H} a_{\mathfrak{q},h}h \in O_{k_\mathfrak{q}}[H]^*$. On demande que pour le caractère trivial χ_0 on obtienne 1. Ceci impose que $f(\chi_0)$ est une unité de k, on peut donc le supposer égal à 1, quitte à modifier tous les $\sum_{h\in H} a_{\mathfrak{q},h}h$. On en déduit que la fonction f est caractérisée par sa valeur en un caractère non trivial de H, valeur appartenant à $k^{(\ell)}$. Exploitons maintenant la condition sur les éléments de l'algèbre de groupe. On choisit χ un caractère non trivial (représentant donc la seconde orbite de R_H pour l'action de Ω). Pour les places premières à ℓ, $O_k[H]$ est localement un ordre maximal. La condition que l'on obtient dit simplement $\sum_{h\in H} a_{\mathfrak{q},h} = 1$ et n'implique rien d'autre pour $\chi\left(\sum_{h\in H} a_{\mathfrak{q},h}h\right)$ que d'être une unité de $O_{k_\mathfrak{q}}[\zeta_\ell)]$. Pour les places au-dessus de ℓ, il n'en va pas de même. On a le produit fibré suivant où l'isomorphisme est assuré par l'hypothèse (H) :

$$\begin{array}{ccc}
O_{k_\mathfrak{q}}[H] & \longrightarrow & O_{k_\mathfrak{q}}[\zeta_\ell] \\
\downarrow & & \downarrow \\
O_{k_\mathfrak{q}} & \longrightarrow & O_{k_\mathfrak{q}}/\ell \simeq O_{k_\mathfrak{q}}[\zeta_\ell]/(1-\zeta_\ell)
\end{array}$$

Le morphisme de la ligne du haut est l'évaluation en χ, celui de la colonne de gauche, l'évaluation en χ_0, ceux de la ligne du bas et de la colonne de droite les passages au quotient. Comme le morphisme de la ligne du bas est surjectif sur les éléments inversibles, la condition de Milnor [M] est vérifiée et le sous-groupe de $O_{k_\mathfrak{q}}[H]^*$ des éléments dont l'image par χ_0 est 1 est isomorphe au groupe $U^{(1)}(O_{k_\mathfrak{q}}[\zeta_\ell])$ des unités de $O_{k_\mathfrak{q}}[\zeta_\ell]$ congrues à 1 mod $(1-\zeta_\ell)$. Finalement, le groupe $\mathcal{G}$ est isomorphe à $k^{(\ell)}\prod_{(\mathfrak{q},\ell)=1} U(O_{k_\mathfrak{q}}[\zeta_\ell])\prod_{\mathfrak{q}|\ell} U^{(1)}(O_{k_\mathfrak{q}}[\zeta_\ell])$.

Le groupe noyau recherché est donc

$$J(k^{(\ell)}/k^{(\ell)}\prod_{(\mathfrak{q},\ell)=1} U(O_{k_\mathfrak{q}}[\zeta_\ell])\prod_{\mathfrak{q}|\ell} U^{(1)}(O_{k_\mathfrak{q}}[\zeta_\ell]),$$

ce qui montre que :

THÉORÈME 3. — *La classe de O_N se trouve dans un sous-groupe de* $\mathrm{Cl}(O_k[H])$ *isomorphe au groupe des classes généralisées de $k^{(\ell)}$ de rayon* $(1-\zeta_\ell)$.

Bien entendu, si on fait une extension des scalaires à l'ordre maximal $\mathcal{M}$, la classe de $(\mathcal{M}O_N)$ est caractérisée par un élément de $\mathrm{Cl}(O_k[\zeta_\ell])$.

3. Construction de l'invariant

On se réfère à [F], le $O_k[H]$-module O_N est représenté par l'application $\chi \in R_H \mapsto \left(\frac{<a_{\mathfrak{q}},\chi>}{<\theta,\chi>}\right)_{\mathfrak{q}}$. Le rappel du § 1 montre que ceci peut être choisi égal à 1 pour toutes les places premières à p. Tenant compte du § 2, on se restreint aux caractères non triviaux de H. Le $\mathcal{M}$-module $\mathcal{M}O_N$ est libre si et seulement si les idéaux I_χ (de valuation nulle en dehors de p et engendrés en $\mathfrak{P}_i$ par $\left(\frac{<a_{\mathcal{P}},\chi>}{<\theta,\chi>}\right)_{\mathfrak{q}}$ sont principaux ; ces idéaux étant conjugués (l'application est Ω-équivariante), il suffit de le montrer pour un seul d'entre eux. On calcule la valuation $v_{\mathfrak{P}_i}\left(\left(\frac{<a_{\mathcal{P}},\chi>}{<\theta,\chi>}\right)_{\mathfrak{q}}\right)$ et pour cela la valuation en $\mathfrak{P}_i''$ (resp. $\mathfrak{P}_i'$) de $< a_{\mathcal{P}},\chi >$ (resp. $< \theta,\chi >$). Ceci est facilité par les hypothèses de ramification en p : θ est une base normale entière de $K^{(\ell)}/\mathbb{Q}^{(\ell)}$ et $a_{\mathcal{P}}$ une base normale entière locale en $\mathfrak{P}_i'$ de $N^{(\ell)}/k^{(\ell)}$, ces extensions étant des extensions de Kummer les valuations cherchées se déduisent du théorème 8 de [F]. On fixe i, χ le caractère de H, on note $\mathfrak{p}$, $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$ les idéaux qui interviennent. Rappelons le calcul :

Soit A, (resp. A') l'application d'Artin de $J(k^{(\ell)})$ (resp. $\mathbb{Q}^{(\ell)}$) dans $\mathrm{Gal}(N^{(\ell)}/k^{(\ell)})$ (resp. $\mathrm{Gal}(K^{(\ell)}/\mathbb{Q}^{(\ell)})$), on peut restreindre ces applications à $U_{\mathfrak{P}}$ (resp. $U_{\mathfrak{p}}$), comme la ramification est modérée et totale en ces places A et A' restent surjectives et leur noyaux contiennent respectivement $U_{\mathfrak{P}}^{(1)}$, $U_{\mathfrak{p}}^{(1)}$. On compose ces restrictions avec le caractère χ, puis on réduit modulo $\mathfrak{p}$ (comme $p \equiv 1 \bmod \ell$, la réduction est injective sur le groupe des racines ℓ-èmes de l'unité). On a finalement construit deux applications. $\chi_{\mathfrak{P}}$. $\chi_{\mathfrak{p}}$:

$$\chi_{\mathfrak{P}} \ : \mathbb{F}_p^* \simeq U_{\mathfrak{P}}/U_{\mathfrak{P}}^{(1)} \longrightarrow < \zeta_\ell > \subset \mathbb{F}_p^* \qquad \chi_{\mathfrak{p}} \ : \mathbb{F}_p^* \simeq U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)} \longrightarrow < \zeta_\ell > \subset \mathbb{F}_p^*$$

Comme $\mathbb{F}_p^*$ est cyclique, ces morphismes sont des élévations à une certaine puissance. Il existe donc deux entiers $1 \leqslant r(\chi), r'(\chi) < \ell$ tels que pour $u \in \mathbb{F}_p^*$ on ait :

$$\chi_{\mathfrak{P}}(u) = u^{-\frac{p-1}{\ell}r(\chi)} \qquad \chi_{\mathfrak{p}}(u) = u^{-\frac{p-1}{\ell}r'(\chi)}$$

La théorie du corps de classes nous donne la commutation du diagramme suivant :

$$\begin{array}{cccccc} \chi_{\mathfrak{P}} & : & \mathbb{F}_p \simeq U_{\mathfrak{P}}/U_{\mathfrak{P}}^{(1)} & \longrightarrow & <\zeta_\ell>\subset \mathbb{F}_p^* \\ & & \downarrow & & \downarrow \\ \chi_{\mathfrak{p}} & : & \mathbb{F}_p \simeq U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)} & \longrightarrow & <\zeta_\ell>\subset \mathbb{F}_p^* \end{array}$$

où la flèche verticale de droite est l'identité et celle de gauche induite par la norme revient à l'élévation à la puissance $n = [k : \mathbb{Q}]$. On en déduit une relation entre $r(\chi)$ et $r'(\chi)$:

$$\chi_{\mathfrak{P}}(u) = u^{-\frac{p-1}{\ell}r(\chi)} = \chi_{\mathfrak{p}}(u^n) = u^{-p^b n_0 \frac{p-1}{\ell} r'(\chi)}$$

Mais $u^p = u$ dans $\mathbb{F}_p$, il reste donc $\frac{p-1}{\ell}r(\chi) = n_0\frac{p-1}{\ell}r'(\chi) \bmod p-1$, ce qui donne $r'(\chi) = [r(\chi)t]_\ell$ où t est l'inverse de n_0 mod ℓ et $[\ ]_\ell$ désigne le reste dans la division euclidienne par ℓ. Le théorème 8 de [F] affirme que :

THÉORÈME 4. — [F] *On a les égalités :*

$$v_{\mathfrak{P}''}(< a_{\mathcal{P}}, \chi >) = r(\chi) \qquad v_{\mathfrak{P}'}(< \theta, \chi >) = r'(\chi).$$

On en déduit $v_{\mathfrak{P}''}(< \theta, \chi >) = r'(\chi)n = r'(\chi)p^b n_0$ puis $v_{\mathfrak{P}''}\left(\frac{<a_{\mathcal{P}},\chi>}{<\theta,\chi>}\right) = r(\chi) - [r(\chi)t]_\ell p^b n_0 \equiv 0 \bmod \ell$ ce qui nous donne :

$$v_{\mathfrak{P}}\left(\frac{< a_{\mathcal{P}}, \chi >}{< \theta, \chi >}\right) = \frac{1}{\ell}\left(r(\chi) - [r(\chi)t]_\ell p^b n_0\right).$$

On note s_α les automorphismes de $\mathrm{Gal}(N^{(\ell)}/N) \simeq \mathrm{Gal}(\mathbb{Q}^{(\ell)}/\mathbb{Q})$ définis par $s_\alpha(\zeta_\ell) = \zeta_\ell^\alpha$ pour $\alpha \in \{1, ..., \ell-1\}$, on peut énoncer :

COROLLAIRE 1. — *La décomposition de l'idéal I_χ en idéaux premiers est :*

$$I_\chi = \prod_{\alpha\in\{1,\ldots,\ell-1\}} s_\alpha^{-1}(\mathfrak{P})^{\frac{1}{\ell}(\alpha-[\alpha t]_\ell n_0 p^b)}$$

Démonstration. — Il suffit de remarquer que

$$v_{s_\alpha^{-1}(\mathfrak{P})}\left(\frac{< a_{\mathcal{P}}, \chi >}{< \theta, \chi >}\right) = v_{\mathfrak{P}}\left(s_\alpha\left(\frac{< a_{\mathcal{P}}, \chi >}{< \theta, \chi >}\right)\right) = v_{\mathfrak{P}}\left(\frac{< a_{\mathcal{P}}, \chi^\alpha >}{< \theta, \chi^\alpha >}\right).$$

Pour obtenir cette valuation, il suffit de remplacer $r(\chi)$ par $\alpha r(\chi)$ dans la formule précédent le théorème 4, on peut donc, quitte à remplacer le caractère χ par un conjugué, supposer que $r(\chi) = 1$ et on obtient la formule de l'énoncé.

Remarque. — L'idéal I_χ est ambige dans $k^{(\ell)}/\mathbb{Q}^{(\ell)}$.

COROLLAIRE 2. — *L'idéal $I_\chi s_{-1}(I_\chi)$ est égal à $\frac{\mathcal{P}}{p}O_{k^{(\ell)}}$.*

Démonstration. — D'après le théorème précédent on a :

$$\begin{aligned}
I_\chi s_{-1}(I_\chi) &= \prod_{\alpha\in\{1,\dots,\ell-1\}} s_\alpha^{-1}(\mathfrak{P})^{\frac{1}{\ell}\left(\alpha-[\alpha t]_\ell n_0 p^b+\ell-\alpha-[(\ell-\alpha)t]_\ell n_0 p^b\right)} \\
&= \prod_{\alpha\in\{1,\dots,\ell-1\}} s_\alpha^{-1}(\mathfrak{P})^{\frac{1}{\ell}(\ell-\ell p^b n_0)} \\
&= \prod_{\alpha\in\{1,\dots,\ell-1\}} s_\alpha^{-1}(\mathfrak{P})^{(1-p^b n_0)} = \mathcal{P}^{1-n}O_{k^{(\ell)}} = \frac{\mathcal{P}}{p}O_{k^{(\ell)}}
\end{aligned}$$

COROLLAIRE 3. — *Si $\mathcal{M}O_N$ est $\mathcal{M}$-libre (et a fortiori si O_N est $\mathbb{Z}[H]$-libre) l'idéal $\mathcal{P}O_{k^{(\ell)}}$ est principal.*

Démonstration. — Le second paragraphe montre en effet que I_χ est alors principal.

COROLLAIRE 4. — *Si c est la conjugaison complexe dans $k^{(\ell)}/\mathbb{Q}$ l'idéal $I_\chi \mathrm{c}(I_\chi)$ est principal.*

Démonstration. — Si k est totalement réel, il n'y a rien à démontrer car alors $s_{-1} = \mathrm{c}$. Si k n'est pas totalement réel, la conjugaison complexe dans $k^{(\ell)}/\mathbb{Q}$ est le produit de s_{-1} et de l'automorphisme de $k^{(\ell)}/\mathbb{Q}^{(\ell)}$ d'ordre 2, or ce dernier a une action triviale sur I_χ. $\square$

Ce corollaire permet facilement de construire des exemples d'extensions relatives modérément ramifiées sans base normale d'entiers.

Exemple. — Soit K l'extension cubique de $\mathbb{Q}$ ramifiée uniquement en 7, $k/\mathbb{Q}$ une extension de degré 7, ramifiée en 7 et 29, $N = Kk$; le $O_k[H]$-module O_N n'est pas libre. S'il l'était, $\mathcal{P}O_{k^{(3)}}$ serait principal ; en prenant la norme sur k, $\mathcal{P}^2$ serait principal. Comme $\mathcal{P}$ est ramifié dans $k/\mathbb{Q}$, l'ordre de sa classe divise 7, d'où $\mathcal{P}$ principal. Montrons que ce n'est pas le cas. Soit $k'/\mathbb{Q}$ la sous-extension de $\mathbb{Q}^{(29)}$ de degré 7, $k''/\mathbb{Q}$ la sous-extension de $\mathbb{Q}^{(49)}$ de degré 7 ; k est un sous-corps de $k'k''$. Comme $7^7 \equiv 1 \bmod 29$, le degré résiduel de 7 dans $\mathbb{Q}^{(29)}$ est égal 7, cet idéal est donc inerte dans $k'/\mathbb{Q}$, il est totalement ramifié dans $k''/\mathbb{Q}$, on en déduit que l'idéal premier au-desus de 7 dans $k/\mathbb{Q}$ est inerte dans l'extension non ramifiée $k'k''/k$, son ordre dans le groupe des classes de k est multiple de 7.

Faisons maintenant le lien avec les sommes de Gauss. Puisque les idéaux $\mathfrak{p}_i$ sont totalement ramifiés dans $k^{(\ell)}/\mathbb{Q}^{(\ell)}$, l'idéal I_χ^n est l'étendu à $k^{(\ell)}$ de l'idéal J_χ de $\mathbb{Q}^{(\ell)}$ défini par :

$$J_\chi = \prod_{\alpha=1}^{\ell-1} s_\alpha^{-1}(\mathfrak{p})^{\frac{1}{\ell}\left(\alpha-[\alpha t]_\ell n_0 p^b\right)}$$

Soit $\mathbb{Q}^{(p)}$ le p-ème corps cyclotomique, on note $\check{\mathcal{P}}$ (resp. $\check{\mathfrak{P}}$) l'unique idéal premier de $\mathbb{Q}^{(p)}$ (resp. $\mathbb{Q}^{(p\ell)}$) au-dessus de p (resp. $\mathfrak{p}$). La réduction modulo $\mathfrak{p}$ est injective sur le groupe des racines $p-1$-ème de l'unité. Soit ω le caractère de Teichmuller de $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^* \simeq \mathrm{Gal}(\mathbb{Q}^{(p)}/\mathbb{Q}) \to \mu_{p-1}$. On choisit $\chi = \omega^{-\frac{p-1}{\ell}}$, c'est un caractère engendrant $\widehat{\mathrm{Gal}(K/\mathbb{Q})}$. On rappelle les résultats bien connus ([L], ch. 1, §2, théorème 2.2). La somme de Gauss $\tau(\chi)$ appartient à $K^{(\ell)} \subset \mathbb{Q}^{(p\ell)}$ et admet dans $\mathbb{Q}^{(p\ell)}$ la décomposition suivante en produit d'idéaux premiers (on prend la formulation et les notations de [L], th. 2.2 avec $k = \frac{p-1}{\ell}$) :

$$\tau(\chi)\mathbb{Z}[\zeta_{p\ell}] = \prod_{\alpha=1}^{\ell-1} s_\alpha^{-1}(\check{\mathfrak{P}})^{(p-1)<\frac{\alpha}{\ell}>}.$$

On en déduit, puisque n et ℓ sont premiers entre eux que :

$$\tau(\chi^t)^n\mathbb{Z}[\zeta_{p\ell}] = \prod_{\alpha=1}^{\ell-1} s_\alpha^{-1}(\check{\mathfrak{P}})^{(p-1)<\frac{t\alpha}{\ell}>n}.$$

Le quotient $\tau(\chi)/\tau(\chi^t)^n$ qui appartient à $\mathbb{Q}^{(\ell)}$ a une décomposition en idéaux premiers dans $\mathbb{Q}^{(p\ell)}$ égale à :

$$\prod_{\alpha=1}^{\ell-1} s_\alpha^{-1}(\check{\mathfrak{P}})^{(p-1)(<\frac{\alpha}{\ell}>-<\frac{t\alpha}{\ell}>n)}.$$

On en déduit, dans $\mathbb{Q}^{(\ell)}$:

$$J_\chi = \left(\frac{\tau(\chi)}{\tau(\chi^t)^n}\right) = \prod_{\alpha=1}^{\ell-1} s_\alpha^{-1}(\mathfrak{p})^{\frac{1}{\ell}(\alpha-[t\alpha]_\ell n)}$$

4. Calculs dans le groupe des classes de $k^{(\ell)}$

On reprend la démarche de [C]. utilisant le fait que I_χ est un idéal ambige de $k^{(\ell)}/\mathbb{Q}^{(\ell)}$ annulé par $1+\mathrm{c}$ pour montrer que si $\mathcal{M}O_N$ est $\mathcal{M}$-libre, $[k:\mathbb{Q}]$ est une puissance de 2.

On veut évaluer le nombre de classes de $k^{(\ell)}$ représentées par des idéaux ambiges et annulées par $1+\mathrm{c}$. On note C_1 le groupe des classes de $k^{(\ell)}$

représentées par des idéaux ambiges dans $k^{(\ell)}/\mathbb{Q}^{(\ell)}$ et C_1^- le sous-groupe de C_1 annulé par $1+\mathrm{c}$. On commence par décomposer C_1 en sa composante paire et sa composante impaire : $C_1 = C_{1,\text{pair}} \bigoplus C_{1,\text{impair}}$; la composante $C_{1,\text{impair}}$ s'obtient par $\mathbb{Z}[\frac{1}{2}] \otimes_{\mathbb{Z}} C_1$ et les idempotents $\frac{1+\mathrm{c}}{2}$, $\frac{1-\mathrm{c}}{2}$ opèrent sur elle, le sous-groupe

$$\mathcal{C} = \frac{1-c}{2} Z[\frac{1}{2}] \otimes_Z C_1$$

est formé des classes représentées par des idéaux ambiges, d'ordre impair et annulées par $1+\mathrm{c}$. On peut calculer l'ordre de ce groupe en utilisant les arguments développés par G. Gras [G]. On rappelle celles des suites exactes de C. Chevalley conduisant à la formule des classes ambiges et dont nous avons besoin. On utilise les notations suivantes :

Pour chaque corps L, on désigne par I_L (resp. P_L) le groupe des idéaux fractionnaires (resp. fractionnaires et principaux) de L. Rappelons que G est le groupe de Galois de k/Q, isomorphe à $\mathrm{Gal}(k^{(\ell)}/Q^{(\ell)})$; on note j l'injection des idéaux de $Q^{(\ell)}$ dans $k^{(\ell)}$. Le groupe C_1 peut être défini par l'isomorphisme :

$$C_1 \simeq \frac{I^G_{k^{(\ell)}}}{I^G_{k^{(\ell)}} \cap P_{k^{(\ell)}}} \simeq \frac{I^G_{k^{(\ell)}}}{P^G_{k^{(\ell)}}}$$

Les suites exactes suivantes permettent de décrire ce groupe et d'en donner l'ordre :

$$1 \longrightarrow \frac{I^G_{k^{(\ell)}} \cap P_{k^{(\ell)}}}{j(P_{Q^{(\ell)}})} \longrightarrow \frac{I^G_{k^{(\ell)}}}{j(P_{Q^{(\ell)}})} \longrightarrow \frac{I^G_{k^{(\ell)}}}{I^G_{k^{(\ell)}} \cap P_{k^{(\ell)}}} \longrightarrow 1 \tag{1}$$

$$1 \longrightarrow \mathrm{Cl}(Q^{(\ell)}) \longrightarrow \frac{I^G_{k^{(\ell)}}}{j(P_{Q^{(\ell)}})} \longrightarrow \frac{I^G_{k^{(\ell)}}}{j(I_{Q^{(\ell)}})} \longrightarrow 1 \tag{2}$$

$$\frac{I^G_{k^{(\ell)}} \cap P_{k^{(\ell)}}}{j(P_{Q^{(\ell)}})} \simeq \frac{U^*(k^{(\ell)})}{U(k^{(\ell)})^{\sigma-1}} \simeq H^1(G, U(k^{(\ell)})) \tag{3}$$

où $U^*(k^{(\ell)})$ est le groupe des unités de $k^{(\ell)}$ de norme 1 dans $k^{(\ell)}/Q^{(\ell)}$ et σ un générateur de $\mathrm{Gal}(k^{(\ell)}/Q^{(\ell)})$.

On peut récrire ce quotient :

$$|H^1(G, U(k^{(\ell)}))| = [U(Q^{(\ell)}) : N_{k^{(\ell)}/Q^{(\ell)}}(U(k^{(\ell)}))] \left| \frac{H^1(G, U(k^{(\ell)}))}{H^2(G, U(k^{(\ell)}))} \right|$$

Le second facteur est le quotient de Herbrand de $U(k^{(\ell)})$ considéré comme G-module. Si on note $k_0^{(\ell)}$ le sous-corps réel maximal de $k^{(\ell)}$, son groupe des unités est un sous-G-module d'indice fini dans celui de $k^{(\ell)}$ et a donc même quotient de Herbrand.

La localisation étant un foncteur exact, on peut tensoriser les suites et isomorphismes qui précèdent par $\mathbb{Z}[\frac{1}{2}]$, c'est à dire prendre la partie d'ordre impair de chacun des groupes, puis la composante suivant l'idempotent $\frac{1-c}{2}$. Comme $\mathrm{Gal}(k^{(\ell)}/\mathbb{Q})$ est abélien, cela revient à calculer le quotient de Herbrand de $\mathbb{Z}[\frac{1}{2}] \otimes U(k_0^{(\ell)})^{\frac{1-c}{2}}$ qui est trivial. Dans le même temps $\mathbb{Z}[\frac{1}{2}] \otimes U(\mathbb{Q}^{(\ell)})^{\frac{1-c}{2}}$ est le groupe des racines ℓ-ème de l'unité, qui sont toutes des normes dans $k^{(\ell)}/\mathbb{Q}^{(\ell)}$ puisque $(n, \ell) = 1$.

Finalement, après tensorisation par $\mathbb{Z}[\frac{1}{2}]$ et application de l'opérateur $\frac{1-c}{2}$ le noyau de la suite (1) s'annule et il suffit de regarder l'image de I_χ dans le quotient de (2). Étudions de plus près ce groupe. Il est engendré par les classes des idéaux ramifiés dans $k^{(\ell)}/\mathbb{Q}^{(\ell)}$. Soit $\mathcal{S}$ l'ensemble des idéaux premiers de $\mathbb{Z}$ ramifiés dans $k/\mathbb{Q}$. L'hypothèse (H) fait que $\ell \notin S$. Pour $q \in S$, on pose $q\mathbb{Z}[\zeta_\ell] = \mathfrak{q}_1 \dots \mathfrak{q}_{g_q}$ et $\mathfrak{q}_i O_k[\zeta_\ell] = \mathfrak{Q}_{i,1} \dots \mathfrak{Q}_{i,g_q}$. Le groupe $\frac{I^G_{k^{(\ell)}}}{j(I_{\mathbb{Q}^{(\ell)}})}$ est engendré par les idéaux $\prod_{j=1}^{g_q} \mathfrak{Q}_{i,j}$. C'est donc en fait un produit de groupes cycliques $\mathbb{Z}/e_i\mathbb{Z}$ indicés par les $\mathfrak{q}_i$ où e_i est l'indice de ramification de $q \in S$ dans $k/\mathbb{Q}$:

$$\frac{I^G_{k^{(\ell)}}}{j(I_{\mathbb{Q}^{(\ell)}})} \simeq \left(\prod_{q \in \{S \backslash p\}} \left(\prod_{\mathfrak{q}_i | q} \mathbb{Z}/e_i\mathbb{Z} \right) \right) \left(\prod_{\mathfrak{p}_i | p} \mathbb{Z}/n\mathbb{Z} \right)$$

où chaque groupe entre parenthèses est un $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})]$-module. L'image de I_χ se trouve dans le produit $\prod_{\mathfrak{p}_i|p} \mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/n\mathbb{Z})\left[\mathrm{Gal}(\mathbb{Q}^{(\ell)}/\mathbb{Q})\right]$. Compte-tenu des propriétés de I_χ et des calculs précédents on va regarder son image dans $\left(\mathbb{Z}[\frac{1}{2}] \otimes (\prod_{\mathfrak{p}_i|p} \mathbb{Z}/n\mathbb{Z})\right)^{\frac{1-c}{2}}$. On pose $n = 2^d n'$ avec n' impair, alors :

$$\left(\mathbb{Z}\left[\frac{1}{2}\right] \otimes (\prod_{\mathfrak{p}_i|p} \mathbb{Z}/n\mathbb{Z}) \right)^{\frac{1-c}{2}} \simeq \bigoplus_{i=1}^{\frac{\ell-1}{2}} (\mathbb{Z}/n'\mathbb{Z})\, s_i \frac{1 - s_{-1}}{2}.$$

Posons $\mathfrak{P} = \tilde{\mathfrak{P}}\hat{\mathfrak{P}}$ avec $\tilde{\mathfrak{P}}$ d'ordre une puissance de 2 et $\hat{\mathfrak{P}}$ d'ordre impair. Le groupe admet une base sur $\mathbb{Z}/n'\mathbb{Z}$ formée des $s_i^{-1}\left(\hat{\mathfrak{P}}\right)/s_{-1}s_i^{-1}\left(\hat{\mathfrak{P}}\right)$. Puisque I_χ est annulé par $1 + c$, la partie impaire de l'ordre de la classe de I_χ est égale à 1 si les exposants de

$$\prod_{j=1}^{\frac{\ell-1}{2}} \left(\frac{s_j^{-1}\left(\hat{\mathfrak{P}}\right)}{s_{-1}s_j^{-1}\left(\hat{\mathfrak{P}}\right)} \right)^{\frac{1}{\ell}[-\ell+2j+n([(\ell-j)t]_\ell - [jt]_\ell)]}$$

sont divisible par n'. Si $n' \neq 1$, il y a au plus une valeur de j pour laquelle c'est vrai et donc si $\frac{\ell-1}{2} \neq 1$, I_χ n'est pas principal. S'il n'y a qu'un seul facteur dans le produit, $\ell = 3$, $j = 1$ l'invariant calculé n'est nul que si $n' = 1$. Ceci ramène la démonstration du théorème 1 au cas où n est une puissance de 2.

5. Cas où n est une puissance de 2

On commence par démontrer le théorème 1. La réduction que l'on a effectuée dans le paragraphe précédent permet de simplifier la démonstration de [B2].

On suppose que $n = 2^a$. On va utiliser l'interprétation de l'idéal I_χ au moyen des sommes de Gauss. On suppose I_χ principal et on note α_χ un de ses générateurs. On note $j_\chi = \frac{\tau(\chi)}{\tau(\chi^t)^n}$.

Démonstration du Théorème 1. — Si le $\mathcal{M}$-module $\mathcal{M}O_N$ est libre, il existe une unité $u \in O^*_{k^{(\ell)}}$ telle que $\alpha_\chi^n = j_\chi u$. On applique la conjugaison complexe à cette identité et on divise terme à terme les deux expressions :

$$\left(\frac{\alpha_\chi}{\overline{\alpha}_\chi}\right)^n = \frac{j_\chi}{\overline{j}_\chi}\frac{u}{\overline{u}} = \frac{j_\chi^2}{j_\chi \overline{j}_\chi}\frac{u}{\overline{u}} = \frac{j_\chi^2}{p^{1-n}}\frac{u}{\overline{u}} = p\frac{u}{\overline{u}}j_\chi^2 p^{n-2}. \tag{4}$$

Comme n est pair, on en déduit que $p\frac{u}{\overline{u}}$ est un carré dans $k^{(\ell)}$. Puisque $k^{(\ell)}/\mathbb{Q}$ est abélienne, on peut écrire $u = u_0\mu$ où u_0 est une unité réelle et μ une racine de l'unité, on a donc $\frac{u}{\overline{u}} = \mu^2$.

LEMME. — *Les seules racines de l'unité dans $k^{(\ell)}$ sont les racines 2ℓ-èmes de l'unité.*

Démonstration. — Soit $q = 4$ ou un nombre premier, premier à 2ℓ tel que les racines q-èmes de l'unité soient dans $k^{(\ell)}$. Dans le corps $\mathbb{Q}(\zeta_q, \zeta_\ell)/\mathbb{Q}(\zeta_\ell)$ seul 2 (ou le premier q) est ramifié, or p est totalement ramifié dans $k^{(\ell)}/\mathbb{Q}^{(\ell)}$, donc s'il y a une racine q-ème de l'unité dans $k^{(\ell)}$, c'est que $q = p$ mais alors K devrait être inclus dans $k^{(\ell)}$, ce qui n'est pas le cas. □

Si on remplace u par $u\zeta_\ell^r$, comme ℓ est premier à n, on peut supposer $\epsilon = \frac{u}{\overline{u}} = \pm 1$. En conséquence, p ou $-p$ est un carré dans $k^{(\ell)}$. Les seuls sous-corps quadratiques de $k^{(\ell)}$ sont $\mathbb{Q}(\sqrt{\epsilon p})$, $\mathbb{Q}\left(\sqrt{\epsilon p\left(\frac{-1}{\ell}\right)\ell}\right)$, $\mathbb{Q}\left(\sqrt{\left(\frac{-1}{\ell}\right)\ell}\right)$ or on sait que ℓ n'est pas ramifié dans $k/\mathbb{Q}$ et p l'est.

L'isomorphisme (3) du § 4 associe à un idéal principal (a) de $k^{(\ell)}$ ambige dans $k^{(\ell)}/\mathbb{Q}^{(\ell)}$ la classe dans $\frac{U^*(k^{(\ell)})}{U(k^{(\ell)})^{\sigma-1}}$ de l'unité u définie par $\rho(a) = au$ (avec ρ un générateur de $\mathrm{Gal}(k^{(\ell)}/\mathbb{Q}^{(\ell)})$).

Si $\rho(\alpha_\chi) = \alpha_\chi v$, l'image de $\frac{\alpha_\chi}{\overline{\alpha}_\chi}$ est $\frac{v}{\overline{v}}$ et le raisonnement précédent permet de supposer que $\frac{v}{\overline{v}} = \pm 1$; comme la valeur -1 est obtenue avec l'idéal $(\sqrt{\epsilon p})$, on peut écrire :

$$\frac{\alpha_\chi}{\overline{\alpha}_\chi} = (\sqrt{\epsilon p})^r \beta v$$

avec $r \in \{0,1\}$, $\beta \in \mathbb{Q}^{(\ell)}$, $v \in O^*_{k^{(\ell)}}$ ce qui donne, en élevant à la puissance n :

$$[(\sqrt{\epsilon p})^r \beta v]^n = \frac{j_\chi^2}{p^{1-n}} \frac{u}{\overline{u}}. \tag{5}$$

Soit $w_{\mathfrak{P}}$ la valuation dans $k^{(\ell)}$ associée à l'idéal $\mathfrak{P}$ et prolongeant la valuation $v_{\mathfrak{p}}$ associée à $\mathfrak{p}$, calculons la valuation des deux membres de (5) :

$$n\left(\frac{rn}{2} + nv_{\mathfrak{p}}(\beta)\right) = 2nv_{\mathfrak{p}}(j_\chi) - n(1-n)$$

après division par n, le membre de droite est entier impair, pour que celui de gauche le soit aussi, il faut que $r = 1$, $n = 2$. □

Démonstration du théorème 2. — Pour montrer que O_N n'est pas $O_k[H]$-libre on peut supposer que k est l'un des corps du théorème 1. Procédons comme ci-dessus. La propriété équivaut à l'existence d'un α_χ dans $O_{k^{(\ell)}}$ qui est une unité en dehors de p et une unité $u \in O^*_{k^{(\ell)}}$ tels que :

$$\alpha_\chi \equiv 1 \bmod^* (1-\zeta_\ell) \qquad \alpha_\chi^2 = j_\chi u.$$

On remarque que si $\alpha_\chi \equiv 1 \bmod^* (1-\zeta_\ell)$, $\alpha_\chi \zeta_\ell^r$ vérifie la même propriété et donc, comme précédemment, on peut supposer $\frac{u}{\overline{u}} \in \pm 1$ et (4) devient :

$$\left(\frac{\alpha_\chi}{\overline{\alpha}_\chi}\right)^2 = pj_\chi^2 \frac{u}{\overline{u}}$$

avec $\epsilon = \frac{u}{\overline{u}} \in \pm 1$ on en déduit :

$$\frac{\alpha_\chi}{\overline{\alpha}_\chi} = \mu j_\chi \sqrt{\epsilon p} \equiv 1 \bmod (1-\zeta_\ell) \qquad \text{avec } \mu = \pm 1$$

Si on applique l'automorphisme non trivial de $\mathrm{Gal}(k^{(\ell)}/\mathbb{Q}^{(\ell)})$ à la congruence $\mu j_\chi \sqrt{\epsilon p} \equiv 1 \bmod (1-\zeta_\ell)$ celui de droite est invariant et celui de gauche est transformé en son opposé, cela donne simultanément $\mu j_\chi \sqrt{\epsilon p} \equiv 1 \bmod (1-\zeta_\ell)$ et $\mu j_\chi \sqrt{\epsilon p} \equiv -1 \bmod (1-\zeta_\ell)$ soit $2 \equiv 0 \bmod (1-\zeta_\ell)$, donc $2 \equiv 0 \bmod (\ell)$ soit $\ell = 2$, or ℓ est impair. □